Asian Research Journal of Mathematics

17(6): 46-57, 2021; Article no.ARJOM.72836
ISSN: 2456-477X

Non-binary Nonlinear Error-correcting Codes from Finite Upper Half-planes

Eduardo Brandani da Silva[1*], Maycow G. Carneiro[2] and Frederico Ventura Batista[3]

[1] *Universidade Estadual de Maringá, Av. Colombo, 5790 - Zona 7, Maringá, Paraná, Brazil.*
[2] *Universidade Tecnológica Federal do Paraná, Linha Santa Bárbara, s/n, Francisco Beltrão, Paraná, Brazil.*
[3] *Instituto Federal do Norte de Minas Gerais, Fazenda Varginha Km 02 Rod. Salinas/Taiobeiras - Salinas, Minas Gerais, Brazil.*

Authors' contributions

This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/ARJOM/2021/v17i630308
Editor(s):
(1) Dr. Nikolaos D. Bagis, Aristotle University of Thessaloniki, Greece.
Reviewers:
(1) Low Jie Ying (JESSLYNN), Sultan Idris Education University, Malaysia.
(2) Ali J. Abboud, University of Diyala, Iraq.
Complete Peer review History: http://www.sdiarticle4.com/review-history/72836

Original Research Article

Received: 01 July 2021
Accepted: 02 September 2021
Published: 04 September 2021

Abstract

Current work builds new families of non-binary nonlinear error-correcting codes from Finite Upper Half-Plane $\mathbf{H}_q$, with $q = p^r$ and p a prime number. A fundamental domain is defined to a discrete group $\Gamma \subset GL(2, \mathbb{F}_q)$ acting over $\mathbf{H}_q$. We establish some concepts and results on $\mathbf{H}_q$, such that the geometric properties allow us to get codification and decodification.

Keywords: Nonlinear error-correcting codes; finite upper half plane; fundamental domain.

2010 Mathematics Subject Classification: 11T71, 11T60.

**Corresponding author: E-mail: ebsilva@uem.br;*

1 Introduction

In a linear code we consider as an alphabet a finite field $\mathbb{F}$ with q elements, and the code is a vector subspace of $\mathbb{F}^n$. These codes are the most used error-correcting codes for applications. On the other hand, nonlinear codes have been studied far less than the linear codes, but they contain the optimal error-correcting codes.

In a communication system, the transmitted information is always impaired by the action of a noise acting on the transmission channel. Despite its physical characteristics, noise is treated by a probabilistic model, by specifying its probability density function. Through this characterization the signal to be transmitted is processed in order to control the noise action. A key component of the transmitter is the modulator. For an efficient signal modulation of the signal, the modulator uses a signal constellation which is a finite set associated with a geometric structure. The system is usually modelled on a Euclidean environment. However, environments outside the Euclidean context have proven to be a very promising approach.

One of the most important possibilities is to consider constellations of points in the hyperbolic plane. The paper [1] was the first to propose a communication system with the hyperbolic plane as an environment. The main potential for coding in the hyperbolic plane is the infinitude of essentially distinct tessellations, in contrast to a Euclidean case. After [1], several papers connecting hyperbolic geometry with communication and coding theory have been published, [2], [3], [4], [5], among others. In [6] it is stated that it is possible to devise more efficient error correcting codes, in terms of error probability, if they are elaborated from two-dimensional varieties with genus $g \geq 2$. It is known that the inherent geometry of such surfaces is hyperbolic geometry, [7].

In the mid 1980s, A. Terras [8] defined the finite upper half planes. They are defined over finite fields as analogue of the hyperbolic plane $\mathbf{H}$. In this construction, a finite field of odd characteristic was used as the finite analog of the real line. The analog of the upper half plane was constructed including the square root of a non-square to the finite field. Further, in [9] , [10], finite fields of even characteristic were considered. Several questions were studied by Terras and coworkers, mainly the special functions on these planes ([1], [5]), and finite graphs, in which deep results were obtained. In [11], Tiu and Wallace found an application in coding theory. The authors generated a binary linear code using the norm in this model of Finite Upper Half-Plane. These ideas were generalized in [12] where new quasi-cyclic codes were obtained.

In a different way of [12] and [11], current paper employs Finite Upper Half-Planes $\mathbf{H}_q$, proposed by Terras [8], to build non-binary nonlinear error correcting codes from a fundamental domain of a group $\Gamma \subseteq GL(2, \mathbb{F}_q)$ over $\mathbf{H}_q$. Further, codes with good parameters are obtained when we consider the action of $\Gamma = GL(2, \mathbb{F}_q)$ over $\mathbf{H}_{q^2}$. We get a code with parameters $(n = q, M = q(q^2-1), d = q)$. We also give a decoding method for such codes, which uses the geometric properties of $\mathbf{H}_q$, and requires a relative low number of comparisons when compared to the more classical ML decoder.

The paper is divided as follows: Section 2 presents the main results on finite upper half-planes, both for the case where the finite field has odd characteristic, [8], [13], [14], and for the case where the characteristic is even, [9], [10]. In addition, we prove for the general case some results that were only considered in the odd case in [13] and [14]. These results will be used in current work also for the even case. In Section 3 we prove several algebraic results about the fundamental domains. These results are interesting by themselves. In this section we build new families of non-binary nonlinear codes. Section 4 discusses a decoding method.

2 Finite Upper Half-Plane $\mathbf{H}_q$

If p is a odd prime number, in a sequence of works, Celniker [15], Poulos [16], Celniker et. al.[8], Angel and Velasquez [17], [18], Terras [14], [19] considering $q = p^r$, and $\mathbb{F}_q$ a field with q elements, they introduces the finite upper half-plane H_q. In these works they analyzed the geometric and analytic properties of the Finite Upper Half-Plane, which was obtained by replacing $\mathbb{R}$ by $\mathbb{F}_q$ in the Poincaré Upper Half-Plane model of the hyperbolic plane $\mathbf{H}$. Angel [9] and Evans [10] also consider the cases of fields with even characteristic. We can use the geometric properties of these finite spaces to get new families of non-binary nonlinear codes. For this, let us introduce the definitions and results of the cited articles, which will be used throughout this work.

Let $q = p^r$ be a power of an odd prime and let $\mathbb{F}_q$ be a field with q elements and ς a non-square in $\mathbb{F}_q$. The Finite Upper Half-Plane is defined by

$$H_q = \{x + y\sqrt{\varsigma} | \;\; x, y \in \mathbb{F}_q, \;\; y \neq 0\}.$$

Moreover, if $z = x + y\sqrt{\varsigma}$, then $\overline{z} = x - y\sqrt{\varsigma}$.

In the case of a field with even characteristic, since every element of the field is a square, let θ be a root of an irreducible polynomial $x^2 + tx + n$ over $\mathbb{F}_q$. In this case the Finite Upper Half-Plane is defined by

$$H_q = \{x + y\theta | \;\; x, y \in \mathbb{F}_q, \;\; y \neq 0\}.$$

Since θ is a root of $x^2 + tx + n$ over $\mathbb{F}_{q^2}[x]$, then θ^q is also a root. Thus, $n = \theta\theta^q$ and $t = \theta + \theta^q$, once $x^2 + tx + n = (x + \theta)(x + \theta^q)$ in $\mathbb{F}_{q^2}[x]$. It can be proved that the obtained results are independent of the choice of the irreducible quadratic polynomial. Thus, we construct the field $\mathbb{F}_{2^r}$ where the elements are powers of a primitive element α, with $Tr(\alpha) = 1$. In this case, $x^2 + x + \alpha$ is irreducible over $\mathbb{F}_{2^r}$. We construct the finite upper half-plane H_{2^r} with θ, a root of the polynomial $x^2 + x + \alpha$. In this case, we have $\theta\theta^q = \alpha$ and $\theta + \theta^q = 1$.

Unlike the odd case, if $z = x + y\theta$, we take $\overline{\theta} = \theta^q$ and we define $\overline{z} = x + y\overline{\theta}$. Since most of the properties that we will use are valid for both cases, we define

$$\mathbf{H}_q = \{x + \delta y | \;\; x, y \in \mathbb{F}_q, \;\; y \neq 0\}, \;\; \text{where} \;\; \delta = \begin{cases} \sqrt{\varsigma} & \text{if} \quad \text{q is odd} \\ \theta & \text{if} \quad \text{q is even} \end{cases} \tag{2.1}$$

Therefore, $\mathbf{H}_q$ has $q(q-1)$ elements and for $z \in \mathbf{H}_q$, the real part of z and the imaginary part of z are given, respectively by $Re(z) = x$ and $Im(z) = y$. Further, the norm of z is given by $N(z) = z\overline{z}$. With such concepts, the pseudo-distance is defined:

$$d(z, w) = \frac{N(z - w)}{Im(z)Im(w)}.$$

Such a map cannot be considered a distance since it returns elements from the field $\mathbb{F}_q$ and not elements from $\mathbb{R}$. Consider the linear group $GL(2, \mathbb{F}_q)$ of 2×2 matrices with entries in $\mathbb{F}_q$ and non zero determinants. We can define an action of $GL(2, \mathbb{F}_q)$ over $\mathbf{H}_q$, where for $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2, \mathbb{F}_q)$, we have $g(z) = \frac{az+b}{cz+d}$. Thus, $g(z) \in H_q$. Next result is proved for the odd case in the works quoted. We give the proof also to the even case.

Proposition 2.1. *If $g \in GL(2, \mathbb{F}_q)$, then*

$$d(z, w) = d(g(z), g(w)), \;\; \textit{for all } z, w \in H_q.$$

Proof. Let $z = x+\delta y$ and $w = u+\delta v$ be elements of $\mathbf{H}_q$. Then $Im(z) = y$, $Im(w) = v$, $g(z) = \frac{az+b}{cz+d}$, $g(w) = \frac{aw+b}{cw+d}$, $Im(g(z)) = \frac{(ad-bc)Im(z)}{N(cz+d)}$, $Im(g(w)) = \frac{(ad-bc)Im(w)}{N(cw+d)}$. Thus,

$$\begin{aligned} d(g(z), g(w)) &= \frac{N(g(z) - g(w))}{Im(g(z))Im(g(w))} \\ &= \frac{N\left(\frac{(az+b)(cw+d)-(aw+b)(cz+d)}{(cz+d)(cw+d)}\right)}{\frac{(ad-bc)^2 Im(z)Im(w)}{N(cz+d)N(cw+d)}} \\ &= \frac{N((az+b)(cw+d)-(aw+b)(cz+d))}{(ad-bc)^2 Im(z)Im(w)} \\ &= \frac{N((ad-bc)(z-w))}{(ad-bc)^2 Im(z)Im(w)} \\ &= \frac{N(z-w)}{Im(z)Im(w)} \\ &= d(z,w). \end{aligned}$$

□

As in the Poincaré Upper Half-Plane model, we will define a fundamental domain for a fuchsian group over $\mathbf{H}_q$. Before that, we have to define an order in $\mathbb{F}_q$. Let α be a multiplicative generator of the multiplicative group $\mathbb{F}_q^*$. Then, we consider the order

$$0 < \alpha < \alpha^2 < \alpha^3 < \cdots < \alpha^{q-1}. \tag{2.2}$$

Now, let $\Gamma \subset GL(2, \mathbb{F}_q)$ be a subgroup and let Γ' be the set of all non trivial elements of Γ, that is, the elements which are not multiple of the identity, and let $z_0 \in \mathbf{H}_q$ be an element that is not fixed by any element of Γ'. We define the sets:

$$\begin{aligned} D_\Gamma(z_0) &= \{w \in \mathbf{H}_q \mid d(z_0, w) < d(\gamma(z_0), w), \ \ \forall \gamma \in \Gamma'\}, \\ \overline{D_\Gamma(z_0)} &= \{w \in \mathbf{H}_q \mid d(z_0, w) \leq d(\gamma(z_0), w), \ \ \forall \gamma \in \Gamma'\}. \end{aligned}$$

These sets are the analogues of Dirichlet regions for the finite upper half-plane. Note that we need an element $z_0 \in \mathbf{H}_q$ which is not fixed by any element of Γ'. The following example shows that, in general, such an element does not always exist.

Example 2.1. *Let $q = 2$. Then, $\mathbb{F}_q = \mathbb{F}_2 = \{0, 1\}$. We know that the polynomial $p(x) = x^2+x+1$ is irreducible over $\mathbb{F}_2$. Thus, taking δ as the root of $p(x)$ we can construct the Finite Upper Half-Plane H_2 given by:*

$$H_2 = \{x + \delta y \mid x, y \in \mathbb{F}_2, y \neq 0\} = \{\delta, 1 + \delta\}.$$

Consider the subgroup $K \subset GL(2, \mathbb{F}_2)$, given by

$$K = \{g \in GL(2, \mathbb{F}_2) \mid g(\delta) = \delta\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}.$$

Note that K does not support a point z_0 that is not fixed by elements of K'. However if we consider the subgroup $\Gamma \subset GL(2, F_2)$ given by

$$\Gamma = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\},$$

we have that δ is not fixed by elements of Γ'.

Thus, we can classify the subgroups of $GL(2,\mathbb{F}_q)$ according to the following definition.

Definition 2.1. Let $\Gamma \subset GL(2,\mathbb{F}_q)$ be a subgroup. Then, Γ is a Domain Subgroup in H_q if there is $z_0 \in H_q$ such that $\gamma(z_0) \neq z_0$, for every $\gamma \in \Gamma'$.

Next result helps us define a fundamental domain for $\mathbf{H}_q$.

Lemma 2.2. *Let $\Gamma \subset GL(2,\mathbb{F}_q)$ be a domain subgroup of $\boldsymbol{H}_q$ and $z \in \boldsymbol{H}_q$. Then, there is $\gamma \in \Gamma$, such that $\gamma(z) \in \overline{D_\Gamma(z_0)}$. Besides, if $z, w \in \overline{D_\Gamma(z_0)}$ and $\gamma(z) = w$ for some $\gamma \in \Gamma$, then γ is a trivial element.*

Proof. Given $z \in H_q$ take $\gamma \in \Gamma$ such that

$$d(z_0, \gamma(z)) \leq d(z_0, \gamma'(z)),\ \forall\ \gamma' \in \Gamma.$$

Note that γ exists because Γ is finite. We claim that γ is the element we are looking for. In fact, given $\gamma' \in \Gamma'$ we have:

$$\begin{aligned} d(\gamma'(z_0), \gamma(z)) &= d(z_0, (\gamma')^{-1}(\gamma(z))) \\ &= d(z_0, ((\gamma')^{-1} \circ \gamma)(z)) \\ &\geq d(z_0, \gamma(z)). \end{aligned}$$

Then, $\gamma(z) \in \overline{D_\Gamma(z_0)}$. For the second part of the proof, we will argue for contradiction. Let $z, w \in \overline{D_\Gamma(z_0)}$, such that $\gamma(z) = w$. Suppose $\gamma \in \Gamma'$. We have

$$d(z_0, z) \leq d(\gamma(z_0), z)\,.$$

On the other hand, since $\gamma(z) \in \overline{D_\Gamma(z_0)}$, it follows that

$$\begin{aligned} d(\gamma^{-1}(z_0), z) &= d(z_0, \gamma(z)) \\ &\leq d(\gamma(z_0), \gamma(z)) \\ &= d(z_0, z). \end{aligned}$$

However, if $\gamma \in \Gamma'$ then $\gamma^{-1} \in \Gamma$. Thus, taking into account that $z \in \overline{D_\Gamma(z_0)}$, the above inequality results in a contradiction. Therefore, γ is a trivial element. □

From Lemma 1, $\overline{D_\Gamma(z_0)}$ is almost a fundamental domain for the action of $\Gamma \subset GL(2,\mathbb{F}_q)$ over $\mathbf{H}_q$. It is necessary, in some cases, to remove some elements in order to satisfy all the conditions of the following definition.

Definition 2.2. Let $\Gamma \subset GL(2,\mathbb{F}_q)$ be a domain subgroup of H_q and $z_0 \in \mathbf{H}_q$ an element that is not fixed by any $\gamma \in \Gamma'$. A subset $\mathfrak{D}$ of $\mathbf{H}_q$ is a *Fundamental Domain* for the action of Γ over $\mathbf{H}_q$, if $\mathfrak{D}$ is a minimal (referring to cardinality) subset such that $D_\Gamma(z_0) \subseteq \mathfrak{D} \subseteq \overline{D_\Gamma(z_0)}$, and it satisfies:

1. $\bigcup_{\gamma\in\Gamma} \gamma(\mathfrak{D}) = \mathbf{H}_q$;
2. $\overset{\circ}{\mathfrak{D}} \cap \gamma(\overset{\circ}{\mathfrak{D}}) = \emptyset,\ \ \forall \gamma \in \Gamma'$ where

$$\overset{\circ}{\mathfrak{D}} = \{w \in \mathfrak{D} : d(z_0, w) < d(\gamma(z_0), w), \forall \gamma \in \Gamma'\}.$$

Basically, a fundamental domain will have an element from each γ-orbit. Now we give examples for even q.

Example 2.3. *Let $q = 4$ and consider $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ where α is a generator element of $\mathbb{F}_4$. Then we take $x^2 + x + \alpha$, which is irreducible over $\mathbb{F}_4$, and let δ be a root of this polynomial. Then, we have $\boldsymbol{H}_4 = \{x + \delta y |\ \ x, y \in \mathbb{F}_4,\ \ y \neq 0\}$. Now, let us consider $\Gamma = N = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, a \in \mathbb{F}_4 \right\}$ and $z_0 = 1 + \delta$. We have:*

$$D_\Gamma(z_0) = \{1 + \delta\}, \quad \overline{D_\Gamma(z_0)} = \{1 + \delta, 1 + \delta\alpha, 1 + \delta\alpha^2, \alpha + \delta\alpha, \alpha^2 + \delta\alpha^2\}.$$

If we take $\overline{D_\Gamma(z_0)}$, we have $\bigcup_{\gamma\in\Gamma} \gamma(\overline{D_\Gamma(z_0)}) = \boldsymbol{H}_4$, $\overset{\circ}{\mathfrak{D}} \cap \gamma(\overset{\circ}{\mathfrak{D}}) = \emptyset$, $\forall \gamma \in \Gamma'$. However, since $\Gamma(z_1) = \Gamma(z_3)$ and $\Gamma(z_2) = \Gamma(z_4)$, then $\overline{D_\Gamma(z_0)}$ is not a smallest subset that satisfies all the conditions of the definition, that is, we have to delete some elements. Further, if we consider $\mathfrak{D} = \{1 + \delta,\ \ 1 + \delta\alpha,\ \ 1 + \delta\alpha^2\}$ which is a set with one representative element from each γ-orbit, we now have $\bigcup_{\gamma\in\Gamma} \gamma(\mathfrak{D}) = \boldsymbol{H}_4$ and, since $\overset{\circ}{\mathfrak{D}} = \{1 + \delta\}$, then $\overset{\circ}{\mathfrak{D}} \cap \gamma(\overset{\circ}{\mathfrak{D}}) = \emptyset$, $\forall \gamma \in \Gamma'$. Thus, $\mathfrak{D}$ is a smallest subset which satisfies the required properties. Therefore, we obtain a fundamental domain for the action of Γ over $\boldsymbol{H}_4$.

Example 2.4. *If in the previous example we take $\Gamma = K = \{g \in GL(2, \mathbb{F}_4) |\ g(\delta) = \delta\} = \left\{ \begin{pmatrix} c + d & c\alpha \\ c & d \end{pmatrix}, c, d \in \mathbb{F}_4, cd + d^2 + c^2\alpha \neq 0 \right\}$, δ and $1 + \delta$ will be fixed by every elements of K. Taking $z_0 = \alpha + \delta$, we will have $D_\Gamma(z_0) = \{\alpha + \delta,\ \ \alpha^2 + \delta\}$ and $\overline{D_\Gamma(z_0)} = \{\alpha + \delta, \alpha^2 + \delta, \delta, 1 + \delta\}$. Note that, in this case, we cannot delete any element from $\overline{D_\Gamma(z_0)}$, otherwise the condition (1) from Definition 2 will not be satisfied. In addition, since it is easy to verify that the condition (2) is satisfied, then $\mathfrak{D} = \overline{D_\Gamma(z_0)}$ is a fundamental domain for the action of $\Gamma = K$ over $\boldsymbol{H}_4$.*

Examples for the case when q is odd may be found in [14], [20], [13].

Let $z_1, z_2, z_3 \in \mathbf{H}_q$ be three different elements. The cross-ratio is the map given by

$$T(z, z_1, z_2, z_3) = \frac{(z - z_1)(z_2 - z_3)}{(z - z_3)(z_2 - z_1)}.$$

Considering this map and taking $\mathbb{F}_{q^2} = \mathbb{F}_q(\delta)$, where δ is given in (2.1), we get the following result.

Proposition 2.2. *Given different elements $z_1, z_2, z_3 \in \boldsymbol{H}_q$ and different elements $u_1, u_2, u_3 \in \boldsymbol{H}_q$, there is $\gamma \in GL(2, \mathbb{F}_{q^2})$, such that $\gamma(z_1) = u_1$, $\gamma(z_2) = u_2$ and $\gamma(z_3) = u_3$. Moreover, γ is unique up to multiplication by constant, and it can be represented by*

$$\begin{pmatrix} \left(\frac{u_1(z_2 - z_1)}{(u_1 - u_3)(u_2 - u_1)} - \frac{u_3(z_2 - z_3)}{(u_1 - u_3)(u_2 - u_3)}\right) & \left(\frac{u_3 z_1(z_2 - z_3)}{(u_1 - u_3)(u_2 - u_3)} - \frac{u_1 z_3(z_2 - z_1)}{(u_1 - u_3)(u_2 - u_1)}\right) \\ \left(\frac{u_1(z_2 - z_1)}{(u_1 - u_3)(u_2 - u_1)} - \frac{u_3(z_2 - z_3)}{(u_1 - u_3)(u_2 - u_3)}\right) & \left(\frac{u_3 z_1(z_2 - z_3)}{(u_1 - u_3)(u_2 - u_3)} - \frac{u_1 z_3(z_2 - z_1)}{(u_1 - u_3)(u_2 - u_1)}\right) \end{pmatrix}.$$

Proof. Let us consider the cross-ratio maps $T(z, z_1, z_2, z_3) = \frac{(z - z_1)(z_2 - z_3)}{(z - z_3)(z_2 - z_1)}$ and $G(z, u_1, u_2, u_3) = \frac{(z - u_1)(u_2 - u_3)}{(z - u_3)(u_2 - u_1)}$. Taking $\gamma = G^{-1} \circ T$, we have $\gamma(z_1) = u_1$, $\gamma(z_2) = u_2$ and $\gamma(z_3) = u_3$, as well as the given expression. For unicity, let $\gamma' \in GL(2, \mathbb{F}_{q^2})$ be other map such that $\gamma'(z_1) = u_1$, $\gamma'(z_2) = u_2$ and $\gamma'(z_3) = u_3$. Then, z_1, z_2, z_3 are three different elements of $\mathbf{H}_q$ fixed by $\gamma^{-1} \circ \gamma'$. Now, we observe that $z \in \mathbf{H}_q$ is a fixed element if, and only if, $\frac{az + b}{cz + d} = z$, which clearly have three solutions if, and only if, $a = d$ e $b = c = 0$. Thus, it follows that $\gamma' = a\gamma$, $a \in \mathbb{F}_{q^2}$. □

In [14], Γ-tesselations are considered when $q = p^r$, with $r > 1$ and $\Gamma \subseteq GL(2, \mathbb{F}_p)$ for the odd case. We will also consider the even case in the construction of our codes. Further, we may consider $\Gamma = GL(2, \mathbb{F}_q)$ acting over $\mathbf{H}_{q^2}$ both for odd and even q, and that the codes we obtain when we do this are the best for our construction method.

3 A Family of Codes from $\mathbf{H}_q$

Let us consider $\mathbf{H}_q$ as in (2.1) and $\mathfrak{D}$ a fundamental domain for the action of a domain subgroup $\Gamma \subset GL(2,\mathbb{F}_q)$ over $\mathbf{H}_q$. We also consider the order given in (2.2), and we order the elements of $\mathbf{H}_q$ in the following way: given $z = x + \delta y$, $w = u + \delta v \in \mathbf{H}_q$, then $z < w$ if, and only if, $x < u$ or $y < v$ and $x = u$.

Now, we consider the elements of the fundamental domain $\mathfrak{D}$ in ascending order, that is, let $z_1 < z_2 < \cdots < z_n$ be the elements of $\mathfrak{D}$ in the given order. We take the vector $c_0 = [z_1, z_2, \ldots, z_n]$, where $n = |\mathfrak{D}|$. Such a vector will be the generator vector of our code.

To obtain the codewords, let $\gamma \in \Gamma$, and apply it in every entry of c_0. From the examples in the previous section, we may have $\gamma_i(c_0) = \gamma_j(c_0)$, for which it is sufficient that $\gamma_i^{-1} \circ \gamma_j = c.Id$. Then, the code generated by Γ is the set $C = \{c_i\}$, where the codeworks are the distinct elements $c_i = \gamma_i(c_0) = [\gamma_i(z_1), \gamma_i(z_2), \ldots, \gamma_i(z_n)]$.

A code C has parameters (n, M, d), where n is the length, M is the number of codewords and d is the minimum distance of the code, where we are considering the Hamming distance. Some results on such parameters will be obtained.

The length of the code is given by $n = |\mathfrak{D}|$.

Now, considering that $|\Gamma\backslash\mathbf{H}_q|$ represents the number of Γ- orbits generated by the action of Γ in $\mathbf{H}_q$ we have the following:

Proposition 3.1. *Let $\Gamma \subset GL(2,\mathbb{F}_q)$ be a domain subgroup in $\boldsymbol{H}_q$ and $\mathfrak{D}$ be the fundamental domain of the Γ action in H_q. Then, $\mathfrak{D}$ has one and only one representative in each Γ-orbit. Consequently,*

$$|\mathfrak{D}| = |\Gamma\backslash H_q|\,.$$

Proof. Suppose there is a Γ-orbit X such that $X \cap \mathfrak{D} = \emptyset$. Thus, for all $\gamma \in \Gamma$, it follows that $X \cap \gamma(\mathfrak{D}) = \emptyset$. Thus, $X \cap \left(\bigcup_{\gamma\in\Gamma} \gamma(\mathfrak{D})\right) = \emptyset$. This contradicts the fact that $\bigcup_{\gamma\in\Gamma} \gamma(\mathfrak{D}) = H_q$. Therefore, it follows that $\mathfrak{D}$ has a representative of each Γ-orbit generated by the action of Γ in H_q. Now suppose there are u, v belonging to a Γ-orbit Y, so that $u, v \in \mathfrak{D}$. By definition, we have $\mathfrak{D} \subseteq \overline{D_\Gamma(z_0)}$. So $u, v \in \overline{D_\Gamma(z_0)}$. Because u and v belong to the same Γ-orbit Y, there is $\gamma \in \Gamma$ so that $\gamma(u) = v$. Then, by Lemma 2.2, it follows that γ is trivial. Thus, $\gamma(u) = u$, implying $u = v$. Therefore, it follows that $\mathfrak{D}$ has one, and only one, representative of each Γ-orbit. □

According to Burnside's Lemma, for a finite group Γ acting over $\mathbf{H}_q$, if $\mathrm{Fix}(\gamma) = \{z \in \mathbf{H}_q | \gamma(z) = z\}$, then $n = |\mathfrak{D}| = |\Gamma\backslash H_q| = \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma} |\mathrm{Fix}(\gamma)|$. Thus, we are interested in the conjugacy classes of $GL(2,\mathbb{F}_q)$ and determine $\mathrm{Fix}(\gamma)$. Consequently, we will use results from [21] to build the Table 1.

In [14], we have a table for odd q. However, as mentioned early, since in this paper we will consider both cases, we use Table 1.

Proposition 3.2. *Let $\gamma \in GL(2,\mathbb{F}_q)$ and $\boldsymbol{H}_q$ given in (2.1). Then*

$$|Fix(\gamma)| = \begin{cases} q(q-1) & \text{if } \gamma \text{ is of type 1} \\ 0 & \text{if } \gamma \text{ is of type 2 or 3} \\ 2 & \text{if } \gamma \text{ is of type 4} \end{cases}$$

Table 1. Conjugacy Classes of $GL(2,\mathbb{F}_q)$

Type	Representative	# Classes	# Elements in the class
1	$\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$, $a \in \mathbb{F}_q$, $a \neq 0$	$q-1$	1
2	$\begin{bmatrix} a & 1 \\ 0 & a \end{bmatrix}$, $a \in \mathbb{F}_q$, $a \neq 0$	$q-1$	q^2-1
3	$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, $a, b \in \mathbb{F}_q$, $a \neq b$	$\frac{1}{2}(q-1)(q-2)$	$q(q+1)$
4	$\begin{bmatrix} 0 & w^{q+1} \\ -1 & w+w^q \end{bmatrix}$, $w \in \mathbb{F}_{q^2}\backslash\mathbb{F}_q$	$\frac{1}{2}q(q-1)$	$q(q-1)$

Proof. If γ is of type 1, then $\gamma = a.Id$, giving that $\gamma(z) = \frac{az}{a} = z$, that is, $\text{Fix}(\gamma) = \mathbf{H}_q \Rightarrow |\text{Fix}(\gamma)| = q(q-1)$. If γ is of type 2, then $\gamma(z) = z \Leftrightarrow az + 1 = az$, which has no solutions, so $|\text{Fix}(\gamma)| = 0$. Analogously, if γ is of type 3, then $\gamma(z) = z \Leftrightarrow az = bz$ has no solutions, since $a \neq b$. In the case of γ of type 4, we have $\gamma(z) = z \Leftrightarrow z^2 - (w+w^q)z + w^{q+1} = 0$. Now, in (2.1), if q is odd, $\delta = \sqrt{\varsigma}$, where ς is not a square, that is, $x^2 - \varsigma$ is irreducible over $\mathbb{F}_q$, then $\sqrt{\varsigma} \in \mathbb{F}_{q^2}\backslash\mathbb{F}_q$, and we can consider $w = \sqrt{\varsigma}$. Thus, it follows that $w + w^q = 0$, $w^{q+1} = \varsigma$ and then $\pm\sqrt{\varsigma}$ are the solutions of the equation. Since $\pm\sqrt{\varsigma} \in \mathbf{H}_q$, $|\text{Fix}(\gamma)| = 2$. Analogously, if q is even, then, in (2.1), $\delta = \theta$ where θ is the root of an irreducible polynomial $x^2 + tx + n$ over $\mathbb{F}_q$, that is, $\delta \in \mathbb{F}_q^2\backslash\mathbb{F}_q$. Taking $w = \delta$, $w + w^q = t$, $w^{q+1} = n$, then both δ and δ^q are solutions of $z^2 - (w+w^q)z + w^{q+1} = 0$. Since $\delta, \delta^q \in \mathbf{H}_q$, $|\text{Fix}(\gamma)| = 2$. □

As a corollary we have:

Corollary 3.1. *A fundamental domain $\mathfrak{D}$ for the action of $\Gamma = GL(2,\mathbb{F}_q)$ over $\boldsymbol{H}_q$ has only one element.*

Proof. By Burnside's Lemma and from Table 1,

$$\begin{aligned} |\mathfrak{D}| &= |\Gamma\backslash\mathbf{H}_q| \\ &= \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}|\text{Fix}(\gamma)| \\ &= \frac{1}{(q^2-1)(q^2-q)}\left[q(q-1)(q-1) + 0 + 0 + \frac{1}{2}q(q-1)q(q-1)2\right] \\ &= \frac{(q-1)^2(q^2+q)}{(q^2-1)(q^2-q)} \\ &= 1. \end{aligned}$$

□

The corollary shows that we do not get a code when we take $\Gamma = GL(2,\mathbb{F}_q)$ acting on $\mathbf{H}_q$, since we will have $n = 1$.

Example 3.2. *Let us consider the following subgroups*

$$\Gamma_1 = N = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, a \in \mathbb{F}_q \right\},$$

and $\Gamma_2 = K = \{g \in GL(2,\mathbb{F}_q) \mid g(\delta) = \delta\}$. Then, by Table 1 and by Burnside's Lemma, if $\mathfrak{D}_1$ and $\mathfrak{D}_2$ are the fundamental domains of each subgroup, respectively, we have that $|\mathfrak{D}_1| = |\Gamma_1\backslash\boldsymbol{H}_q| = q-1$

and $|\mathfrak{D}_2| = |\Gamma_2 \backslash \boldsymbol{H}_q| = q$. *Now, since* $\boldsymbol{H}_q$ *has* $q(q-1)$ *elements, then if we take* $\mathfrak{D}_1$ *as fundamental domain, we have* q *codewords in our code with minimum distance* q. *Since in this case no element of* $\mathfrak{D}_1$ *is fixed by elements of* $\Gamma_1 = N$, *then the number of codewords is given by* $M = \frac{q(q-1)}{q-1} = q$, *where we take only the distinct codewords. So,* $\gamma_i(z_k) \neq \gamma_j(z_k)$ *and* $d = q-1$. *Thus, we get a code with parameters* $(q-1, q, q-1)$.

If we take $\mathfrak{D}_2$ *as the fundamental domain, we have two elements which are fixed by* γ *of type* 4. *The number of codewords will be* $M = \frac{q(q-1)-2}{q-2} = q+1$ *and the minimum distance will be* $d = q-2$. *Then, we get a code with parameters* $(q, q+1, q-2)$.

The previous example shows that the parameters of the code are not so good since we have a low number of codewords. We can improve the number of codewords for up to $n-1$ times the original number, keeping the same length n and the same minimum distance d, where we are considering the Hamming distance.

Let $c_0 = [z_1, z_2, \ldots, z_n]$ be the generator vector of the code. Taking a right shift in the c_0 by one position in each coordinate, we obtain $n-2$ vectors $c_1 = [z_n, z_1, \ldots, z_{n-1}], \ldots, c_{n-2} = [z_2, z_3, \ldots, z_1]$. Now, if we apply the coding method in these vectors, we have $M(n-1)$ codewords in the new code. We will see later a decoding method different from Maximum Likelihood (ML) method. The method, however, works only for the original code, without an increase in the number of codewords.

On the other hand, if we take a Γ-tessellations, as $\Gamma = GL(2, \mathbb{F}_q)$ acting over $\mathbf{H}_{q^2}$, then we have better results in the parameters and we will be able to keep the decoding method. To analyze this case, we consider the finite fields $\mathbb{F}_q$ and $\mathbb{F}_{q^2} = \mathbb{F}_q(\delta)$ where δ is given in (2.1). In order to build $\mathbf{H}_{q^2}$, we need an element δ_1 which is a root of an irreducible polynomial $x^2 + t_1 x + n_1$ over $\mathbb{F}_{q^2}$ if q is even, or $\delta_1 = \sqrt{\varsigma_1}$ if q is odd, where ς_1 is not a square in $\mathbb{F}_{q^2}$, that is, $\mathbf{H}_{q^2} = \{x + \delta_1 y \mid x, y \in \mathbb{F}_{q^2} = \mathbb{F}_q(\delta), \ \ y \neq 0\}$.

Proposition 3.3. *Let* $\gamma \in GL(2, \mathbb{F}_q)$ *and* $\boldsymbol{H}_{q^2}$ *as above. Then*

$$|Fix(\gamma)| = \begin{cases} q^2(q^2-1) & \text{if} \quad \gamma \ \text{is of type 1} \\ 0 & \text{if} \quad \gamma \ \text{is of type 2, 3 or 4} \end{cases}.$$

Proof. The proof is essentially the same as in Proposition 3.2. Since $|\mathbf{H}_{q^2}| = q^2(q^2-1)$, if γ is of type 1, then $|\mathrm{Fix}(\gamma)| = q^2(q^2-1)$. On other hand, since $\mathbf{H}_{q^2} = \{x + \delta_1 y \mid x, y \in \mathbf{F}_{q^2} = \mathbf{F}_q(\delta), \ \ y \neq 0\}$, the fixed elements for a γ of type 4 is $\pm\delta$ for odd q and $\delta, \ \ \delta^q$ for even q, which does not belong to $\mathbf{H}_{q^2}$. Then, $|\mathrm{Fix}(\gamma)| = 0$. □

Lemma 3.3. *Let* $\mathfrak{D}$ *be a fundamental domain for the action of* $\Gamma = GL(2, \mathbb{F}_q)$ *over* $\boldsymbol{H}_{q^2}$. *Then*

$$|\mathfrak{D}| = |\Gamma \backslash \boldsymbol{H}_{q^2}| = q\,.$$

Proof. The result follows from Burnside's Lemma and from Proposition 3.3. These results show that $|\mathfrak{D}| = \frac{1}{(q^2-1)(q^2-q)}[(q-1)q^2(q^2-1)] = q$. □

Theorem 3.4. *Let* $\mathfrak{D}$ *be a fundamental domain for the action of* $\Gamma = GL(2, \mathbb{F}_q)$ *over* $\boldsymbol{H}_{q^2}$ *and let* $c_0 = [z_1, z_2, \ldots, z_n]$ *be the vector with elements of* $\mathfrak{D}$ *in ascending order. Then, the code* $\mathcal{C} = \{c_i = \gamma_i(c_0) : \gamma_i \in \Gamma, \ \ c_i \neq c_j\}$ *has parameters* $(n = q, M = q(q^2-1), d = q)$.

Proof. The length $n = q$ follows directly from Lemma 3.3. For the number of codewords, since $\mathfrak{D}$ is the fundamental domain, we have $|\mathbf{H}_q| = q^2(q^2-1)$ and, by Proposition 3.3, it follows that $M = \frac{q^2(q^2-1)}{q} = q(q^2-1)$. For minimum distance, if $\gamma \in \Gamma$, then $\gamma^{-1} \in \Gamma$. Now, suppose that there are $\gamma_i, \gamma_j \in \Gamma$ with $\gamma_i(z_k) = \gamma_j(z_k)$ for some $z_k \in \mathfrak{D}$, then z_k is fixed by $\gamma_i^{-1} \circ \gamma_j$. By Proposition

3.3, $\gamma_i^{-1} \circ \gamma_j = c.Id$, so $\gamma_i^{-1} \circ \gamma_j$ fixes every element of $\mathfrak{D}$, that is, $\gamma_i(z_k) = \gamma_j(z_k) \ \ \forall \ \ z_k \in \mathfrak{D}$. Then, $\gamma_i(c_0) = \gamma_j(c_0)$, which is a contradiction since we took distinct codewords. Therefore, the minimum distance will be $d = q$. □

Again, we may observe that, in this case, we are able to increase the number of codewords up to $q-1$ times the original number, by shifting $q-1$ times on the right in the coordinates of the codewords of the original code.

3.1 Decoding method

In order to decode a received codeword $\mathbf{r}$, we will use the Proposition 2.2. Let $\mathbf{e} = [e_1, e_2, \ldots, e_n]$ and $\mathbf{r} = [r_1, r_2, \ldots, r_n]$ be the sent and the received codewords, respectively. Therefore, $\mathbf{e} = \gamma(c_0)$, that is, $e_i = \gamma(z_i), \ \ i = 1, 2, \ldots, n$ for some $\gamma \in \Gamma$. Then, by Proposition 2.2, it is enough to take $r_i, \ \ r_j, \ \ r_k$ and determine $\gamma^{'}$, such that $\gamma^{'}(z_i) = r_i, \ \ \gamma^{'}(z_j) = r_j, \ \ \gamma^{'}(z_k) = r_k$. Next, we verify if $\gamma^{'} \in GL(2, \mathbb{F}_q)$. If not, at least one error has occurred and other combination r_i, r_j, r_k is taken. If $\gamma^{'} \in GL(2, \mathbb{F}_q)$, we verify if $\omega(\gamma^{'}(c_0) - \mathbf{r}) \leq \left\lfloor \frac{d-1}{2} \right\rfloor$, where $\omega(w)$ is the Hamming weight of w. In the affirmative case, the codeword sent is $\mathbf{e} = \gamma^{'}(c_0)$. Otherwise, all three coordinates have an error, and we have to choose other elements r_i, r_j, r_k, all different from those previously chosen. Next, we repeat the procedure.

Since this method corrects up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors, we have to take $q \geq 4$, if $n = d = q$, or $q \geq 5$ if $d = q - 2$. In this case, there will be at least three elements which were sent correctly and by the uniqueness of γ given in the Proposition 2.2, we will be able to determine the correct map γ.

Using this method we have at most $\frac{q(q-1)(q-2)}{6}$ comparisons, if we need to work out all the combinations of $n = q$ elements, taken 3 by 3.

3.2 Comparisons

From Theorem 1, for each q, the parameters of the code are $(q, q(q^2-1), q)$. This implies that for each distance $d = q$ we have only one code. On other hand, we get codes for all distances $d = q$, with also $n = q$, which gives very good parameters, as we see when we compare them with the codes in [22].

4 Conclusions

In this work we introduced the concept of fundamental domain for the finite upper half-plane $\mathbf{H}_q$. This allow us to build new families of non-binary nonlinear error-correcting codes from $\mathbf{H}_q$, for $q = p^r$ and p a prime number. We also establish some concepts and results on $\mathbf{H}_q$, such that its geometric properties give a decodification strategy for these codes.

Competing Interests

Authors have declared that no competing interests exist.

References

[1] Silva EB, Firer M, Costa SR, Palazzo R. Signal constellations in the hyperbolic plane: A proposal for new communication systems. J. Franklin Inst. 2006;343:69-82.

[2] Albuquerque CD, R. Palazzo JR, Silva EB. Topological quantum codes on compact surfaces with genus $g \geq 2$. Journal of Mathematical Physics. 2009;50:023513.

[3] Carvalho ED, Andrade AA. Hyperbolic lattices: A new propose for coding theory. Internat. J. App. Math. 2011;24:65-72.

[4] Lazari H, Palazzo R. Geometrically uniform hyperbolic codes. Comp. Appl. Math. 2005;24(2):173-192.

[5] Blanco-Chacón I, Remón D, Hollanti C, Alsinac M. Nonuniform Fuchsian codes for noisy channels. J. Frankl. Inst. 2014;351:5076-5098.

[6] Cavalcante RG, Lazari H, Lima JD, Palazzo R. A new approach to the design of digital communication systems. AMS-DIMACS Series. 2005;68:145-177.

[7] Cavalcante RG, Palazzo R. Performance analysis of M-PSK signal constellations in Riemannian varieties. Lect. Notes Comp. Science. 2003;2643:191-203.

[8] Celniker N, Poulos S, Terras A, Trimble C, Velasquez E. Is there life on finite upper half planes?. Contemp. Math. 1993;143:65-88.

[9] Angel J. Finite upper half planes over finite fields. Finite Fields and App. 1996;2(1):62-86.

[10] Evans R. Spherical Functions for Finite Upper Half Planes with Characteristic 2. Finite Fields and App. 1995;1(3):376-394.

[11] Tiu PD, Wallace DI. Norm quadratic-residue codes. IEEE Trans. on Inf. Theory. 1994;40(3):946-949.

[12] Silva EB, Castelani EV, Carneiro MG. New quasi-cyclic codes from finite upper half-planes. Int. J. Inf. Coding Th. 2020;5(3-4):239-265.

[13] Shaheen AM. A trace formula for finite upper half planes. J. Ramanujan Math. Soc. 2006;4:343-363.

[14] Terras A. Harmonic analysis on symmetric spaces - Euclidean space, the sphere, and the Poincar upper half-plane. Springer; 2013.

[15] Celniker N. Combinatorial properties of finite, upper half-planes and an improvement on the Tutte polynomial for coloring Cayley graphs. Ph.D. dissertation, UC, San Diego; 1991.

[16] Poulos S. Graph theoretic and spectral properties of finite upper half-planes. Ph.D. Dissertation, UC, San Diego; 1991.

[17] Angel J, Celniker N, Poulos S, Terras A, Trimble C, Velasquez E. Special functions on finite upper half planes. Contemp. Math. 1992;138:1-26.

[18] Angel J, Poulos S, Terras A, Trimble C, Velasquez E. Spherical functions and transforms on finite upper half planes: Eigenvalues of of the combinatorial laplacian, uncertainty, traces. Contemp. Math. 1994;173:15-70.

[19] Terras A. Fourier analysis on finite goups and application. Cambridge Univ. Press; 1999.

[20] Shaheen AM. Finite planes and finite upper half planes: their geometry, a trace formula, modular forms, and Eisenstein series. Ph.D. Dissertation, UC, San Diego; 2005.

[21] Hesbo OEO, Owino MO. On Cunjugacy and order structure of certain classes of finite groups. Int. J. Pure and App. Mat. 2014;91(4):435-458.

[22] Litsyn S, Rains EM, Sloane NJA. Table of nonlinear binary codes. Available:https://www.eng.tau.ac.il/ litsyn/tableand/index.html.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
http://www.sdiarticle4.com/review-history/72836